# DECLARATION OF NIKOLAOS NIKIFORAKIS

**Pursuant to 28 U.S.C. 1746**

## *Qualifications and Experience*

1. My name is Nikolaos (Nick) Nikiforakis. I have a Bachelor's Degree, a Master's Degree, and a PhD, all in Computer Science. My area of research is computer security and privacy. I am an Assistant Professor in the Department of Computer Science at Stony Brook University and I am the director of the PragSec lab, where my students and I perform research in security and privacy. I am the author of more than 40 academic publications in this subject area, which have been cited more than 1100 times. I serve in multiple program committees every year, planning and presenting at the most prestigious computer security conferences. I am the Program Committee co-chair of the Symposium on Electronic Crime Research (eCrime) for 2017. The eCrime conference is a peer-reviewed conference dedicated exclusively to cybercrime studies.

2. I am also the author of the largest technical study of technical support scams (published in the 24th Network and Distributed Systems Symposium, 2017) where my students and I collected and analyzed vast amounts of data on technical support scams. In addition to collecting domain names and phone numbers used by technical support scammers, we also interacted with 60 different scammers while recording the techniques that they used to convince users that their computers were infected with malware, to then convince the consumers to pay substantial sums for unnecessary services.

3. Based on my experience, training, and education, as demonstrated above and as summarized in my current *curriculum vitae*, which is attached hereto as **Nikiforakis Attachment A**, I consider myself to be an expert in computer security and privacy, as well as an expert in identifying scammers posing as qualified and certified technical support providers.

4. Based on my review of the evidence provided by Federal Trade Commission ("FTC") staff in this matter, Troth Solutions engages in conduct that is consistent with my own interactions with technical support scammers. As discussed in more detail below, Troth Solutions utilizes misleading pop-up ads, gains remote access to consumers' computers and then uses information from Windows utilities to falsely claim that the computers are suffering from security or performance issues. Based on these misrepresentations, Troth Solutions convinces consumers that they are in urgent need of technical support, and that the consumers should pay Troth Solutions substantial sums for what is actually unnecessary technical support.

## Analysis of FTC Undercover Calls

### Pre-Call Analysis

5. On January 12, 2017, via FTC's SecureMail platform, I received six audio files of the conversations between the FTC Investigator Roberto Menjivar and various representatives of Troth Solutions. Mr. Menjivar used an undercover identity to conduct an undercover investigation of the purported services provided by Troth Solutions. In addition to these six audio files, I also received official transcriptions of these six audio files and a video file showing the screen of the FTC computer through the end of the first call. Table 1 shows information about these calls and their transcriptions. I have redacted portions of the file names to maintain the confidentiality of the undercover identity used by Investigator Menjivar.

6. On February 1, 2017, I received an encrypted hard drive from the FTC containing forensic images captured from the computer used by Investigator Menjivar during his undercover investigation of the services provided by Troth Solutions. Table 2 shows the disk images contained in the FTC's hard drive together with a brief description of each image.

7. The aforementioned hard drive also contained the following:

    - Video files showing the screen of the computer used to conduct the undercover calls
    - Data captured by Wireshark, a packet analyzer used during each undercover call to monitor network traffic between Troth Solutions and the FTC's computer
    - Memory captured after the end of the undercover call

8. To establish whether the machine that the Troth Solutions representative examined was free from malware, a term that I use to describe viruses and any other type of malicious software, I inspected the 03-Alias.E01 disk image which was the baseline image after it was customized by the FTC. The Troth Solutions representative called Ron inspected this exact same machine during the first call from the FTC investigator.

9. Using both manual (inspecting startup programs, registry, browser add-ons, and installed programs) as well as automated means (scans with two separate antivirus programs, Microsoft Windows Defender and MalwareBytes AntiMalware software) I found no evidence of any malware present on the machine. My search was considerably more thorough than the one performed by the Troth Solutions representatives and I can with certainty state that the issues claimed to be discovered by the Troth Solutions representatives, which are described below in my Call and Transcript Analysis, were not present.

*Table 1. Details of the audio files and transcriptions of the calls between the FTC and Troth Solutions*

| Index | Transcription file name | Corresponding audio file | Duration of audio file |
|---|---|---|---|
| 1 | 01 XXXXX UCP 8005455895 12.08.16.pdf | WS330436.WMA | 00:51:11 |
| 2 | 02 XXXXX UCP 8005455895 12.08.16.pdf | WS330437.WMA | 00:12:43 |
| 3 | 03 XXXXX UCP 8005455895 12.08.16.pdf | WS330438.WMA | 00:16:47 |
| 4 | 04 XXXXX UCP 8005455895 12.08.16.pdf | WS330440.WMA | 00:18:37 |
| 5 | 05 XXXXX UCP 8005455895 12.08.16.pdf | WS330441.WMA | 00:24:05 |
| 6 | XXXXX Voicemail 8005455895 12.08.16.pdf | WS330452.WMA | 00:02:45 |

*Table 2. Forensic disk images available in the hard drive mailed by the FTC*

| Image Name | Description |
|---|---|
| Call #1 / 01-OS Baseline Only.E01 | Forensic image of baseline system configuration used for call to Troth Solutions |
| Call #1 / 02-Baseline Copy.E01 | Forensic duplicate of the above image |
| Call #1 / 03-Alias.E01 | Forensic image created after the customization of the baseline image used for the call to Troth solutions |
| Call #1 / 04-TS-1723018-01-AfterCall.E01 | Forensic image created after the completion of the call by Troth solutions |
| Call #1 / 05-AfterCall(Final).E01 | Forensic image created after the second call from Troth Solutions where a Troth Solutions representative installed one final program (Troth AV Shield) |

## Call and Transcript Analysis

10. In this first call (recording file WS330436.WMA, transcription file 01 XXXXX UCP 8005455895 12.08.16.pdf), the FTC investigator calls Troth Solutions number 1-800-545-5895 where he is greeted by a representative who introduces himself as David. The FTC investigator describes to David that he saw an error message on his computer, which instructed him to call this specific number. David then transfers the FTC investigator to another Troth Solutions representative called Ron who asks some more questions about the investigator's computer and the error message that he received.

11. Even before having a single look at the investigator's computer, Ron claims the following (excerpt from page 8 of transcription file 01 XXXXX UCP 8005455895 12.08.16.pdf):

    *RON: All right. Well, because the problems that you're telling me right now, this kind of problem only comes on a computer if you have some kind of security alert like on your device. That is the only reason when you have these kind of issues on it.*

    *MR. MENJIVAR: I don't -- I don't understand.*

    *RON: Like if you have some kind of a security problem or I would say there are any kind of issues related with any of your other things on your computer, then you would automatically face these kind of problems with it.*

12. The terms "security alert" and "security problem" are very generic terms that cannot convey any one specific meaning. In addition, the representative could have no legitimate way of figuring out that a customer's computer has security issues just because of an alert that the customer saw and described to the representative over the phone. In this instance, of course, the FTC Investigator had not even seen the alert.

13. Ron explains to the investigator that he needs to access his machine to further diagnose the problem. He guides the investigator to the website www.support.me where the investigator downloads a remote administration tool. This tool allows the Troth Solutions representative Ron to have full access to the investigator's computer.

14. Once he gains access, the representative opens up the windows command line tool (cmd.exe), navigates to the root directory of the hard drive C:\ and then executes the command "tree". Tree is a verbose directory listing command which shows all the files and folders present in the directory in which it was executed. The Troth Solutions representative, however, claims that he is running "a quick Microsoft scan" which will show "all the softwares [sic] that you have in this computer." (Page 15 of transcription file 01 XXXXX UCP 8005455895 12.08.16.pdf.) This is a clear misrepresentation of what the tree command does.

15. Once the program ends, the Troth Solutions representative draws attention to the last two statements that are supposedly printed by the program he just ran. *Figure 1* shows that output with two red arrows added to show the output to which Ron refers. These statements are "security expired" and "network hacked." While a non-technical person may believe that these statements came from the "scanning" program the representative claims to have just executed, a person knowledgeable with running programs from the command line will notice that these statements are not printed by the program. Rather, they were typed in by the Troth Solutions representative while the tree program was printing its output. Even putting aside the fact that the tree command, as described earlier, will never print these messages because it is not a security scanner, one can see that the operating system is showing the following two errors right after the sentences pointed to by the red arrows:

- ‘security’ is not recognized as an internal or external command, operable program or batch file
- ‘network’ is not recognized as an internal or external command, operable program or batch file

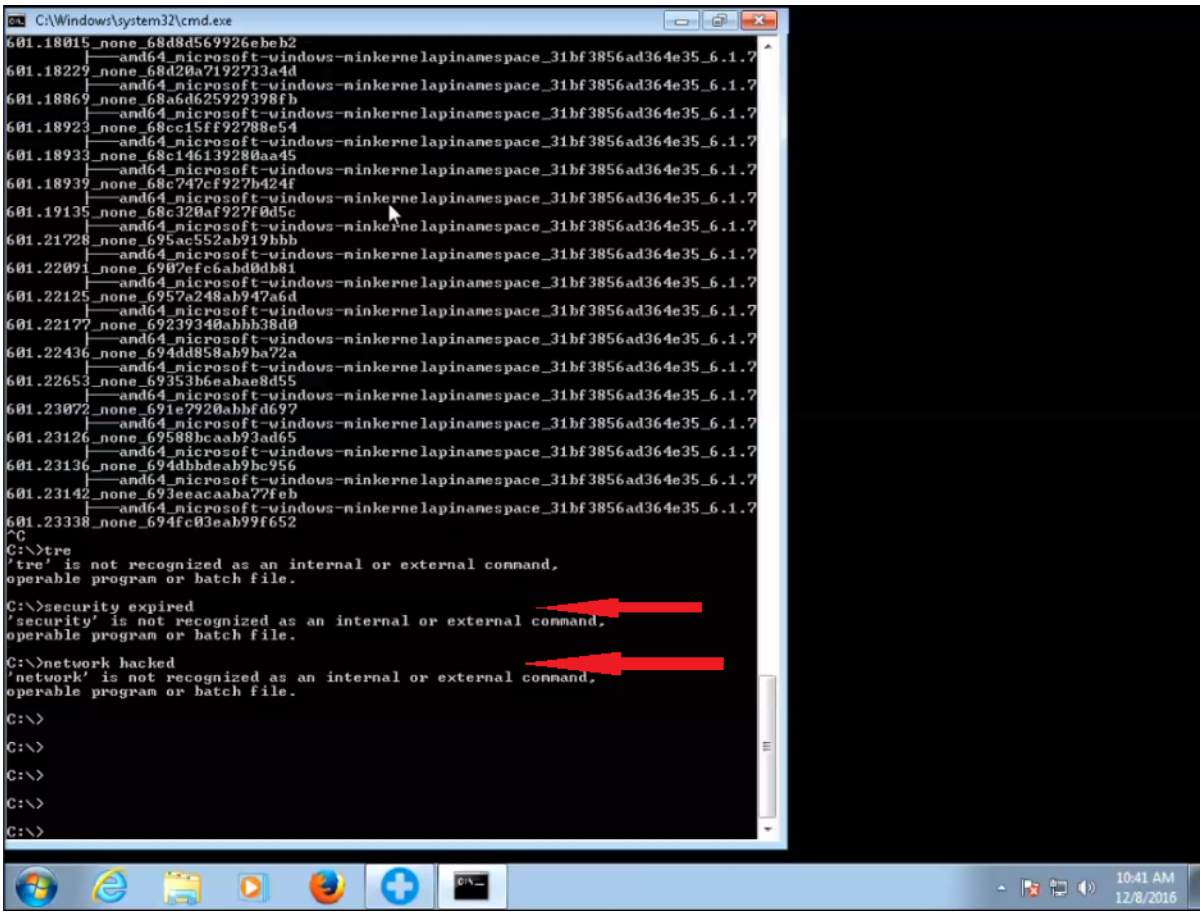


*Figure 1. Screenshot after running the tree command on the investigator's machine. Statements with red arrows are misleading statements typed by the Troth Solutions representative*

16. These errors are generated because the phrases “security error” and “network hacked” were typed in by the Troth Solutions representative who followed each phrase by the “Enter” key. Following standard command-line protocols, Windows tried to find and execute the program “security” with a command line argument “expired” and then the program “network” with the command-line argument “hacked”. Neither of these are programs that are present on a typical Windows system and thus the command-line presents the aforementioned errors. In our study of technical support scams (published in the 24th Network and Distributed Systems Symposium, 2017) my students and I observed that 40% of all the scammers we interacted with, used the same technique to try to convince us that our test machines were infected with malware (when in fact, as in this case, they were not).

17. Even without any more information, at this point, it is clear not only that the Troth Solutions representative is misrepresenting the function of the "tree" command to match his narrative (that of the investigator's machine having security problems) but in fact he manufactures error messages meant to convince the investigator that his computer's security is "expired" (which in itself is a meaningless statement, because a computer's "security" is a property, and unlike software, cannot be described as "expired") and that his network is "hacked."

18. After showing the error messages that he himself typed after the output of the "tree" command, the Troth Solutions representative runs the msconfig program, which is a Windows tool that shows information about the startup programs running in Windows and the Windows services that are currently running or are stopped. The representative goes to the "Services" tab where he shows specific Microsoft services that are listed as "Stopped" and then tells the investigator that these are stopped because they have expired and need to be updated (*Figure 2*). This is a misrepresentation of what these services are and why they are stopped. All Windows installations come with services that are, by default, not running as a way of preserving resources. These services are not "security softwares [sic]" (page 17 of the transcription) and they do not "expire."

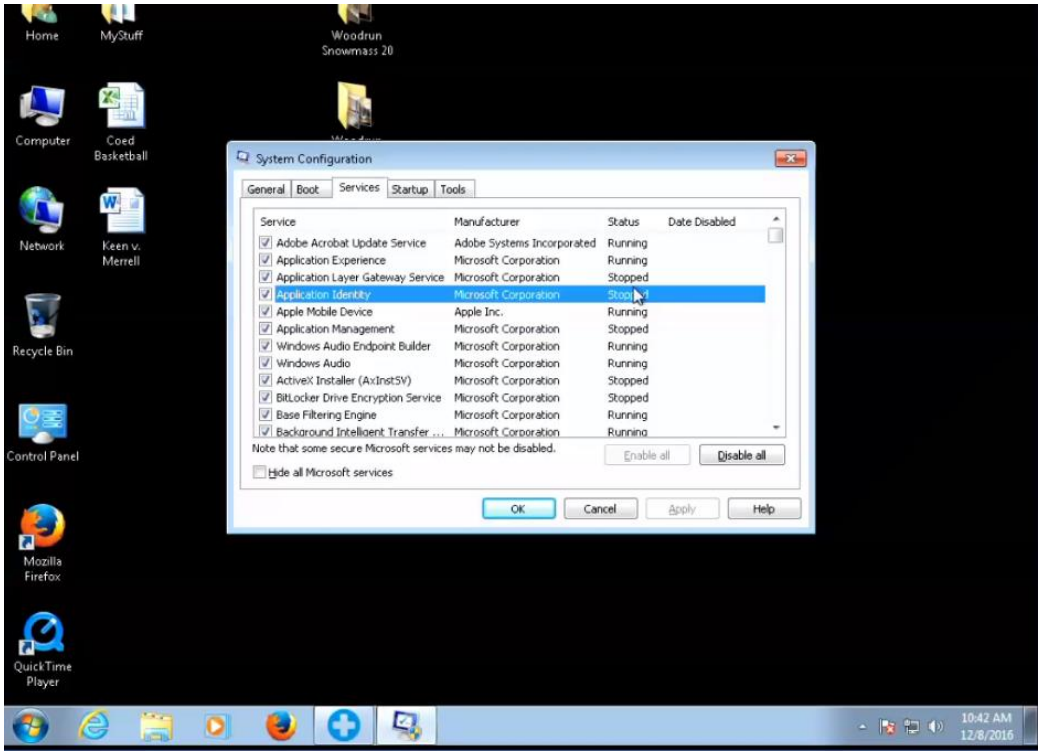


*Figure 2. Services in msconfig that appear as stopped.*

19. The Troth Solutions representative also claims that if this "security" is not installed, the investigator's computer will be "blocked […] because without the security, you're not

authorized to do any kind of banking, shopping, anything personal on your device." (Page 17 of transcription file 01 XXXXX UCP 8005455895 12.08.16.pdf.) Even if these services were somehow related to security (which they are not), a user can still use his own computer even if they have expired. The Troth Solutions representative is falsely claiming that the computer will be blocked to create a sense of urgency, which he can take advantage of in order to later charge the investigator $499 for unnecessary services. In the aforementioned study of technical support scams, my students and I observed that 67% of all the scammers we interacted with, used the same technique to try to convince us that our test machines were infected with malware (when in fact, as in this case, they were not).

**Post-Call Analysis**

20. To understand the services rendered by the Troth Solutions representatives, I analyzed the videos and post-call evidence and identified what the agents did and what software was installed:
    - Download and run malwarebytes anti-malware free trial version
        - No virus or malware was discovered
        - The software was later uninstalled before the agent claimed to have finished her work
    - Execute Windows utilities for finding and repairing corrupt files
        - No issues discovered
    - Added AdblockPlus to Chrome and Firefox
    - Download and execute Junkware removal tool from Malwarebytes
    - Download, install, and execute Microsoft Security Essentials
    - Download, install, and execute CCleaner
    - Download, install, and execute Troth Privacy Shield

21. Notably, the results of the Malwarebytes scan showed that there was no malware present on the machine, directly contradicting the representatives' earlier statements. Most of the software that was downloaded is freely available software (either completely free or in trial forms) from reputable vendors:

    - **MalwareBytes Anti-malware** is an antivirus program that can identify and remove viruses and malware
    - **MalwareBytes Junkware removal tool** removes adware and potentially unwanted programs
    - **CCleaner** removes temporary files and fixes registry issues
    - **Microsoft Security Essentials** is an antivirus program that can identify and remove viruses and malware
    - **AdblockPlus** is ad-blocking software that can be installed in modern web browsers

22. The only proprietary software that the representative downloaded and installed is "Troth Privacy Shield" which is software that Troth Solutions has either developed in house, or has purchased as a generic program and has the rights to brand it. The latter is often referred to as a "white label" product. While I saw no evidence that the software was malicious, four popular antivirus products currently flag it as malware, which is a cause for concern (*Figure 3*).

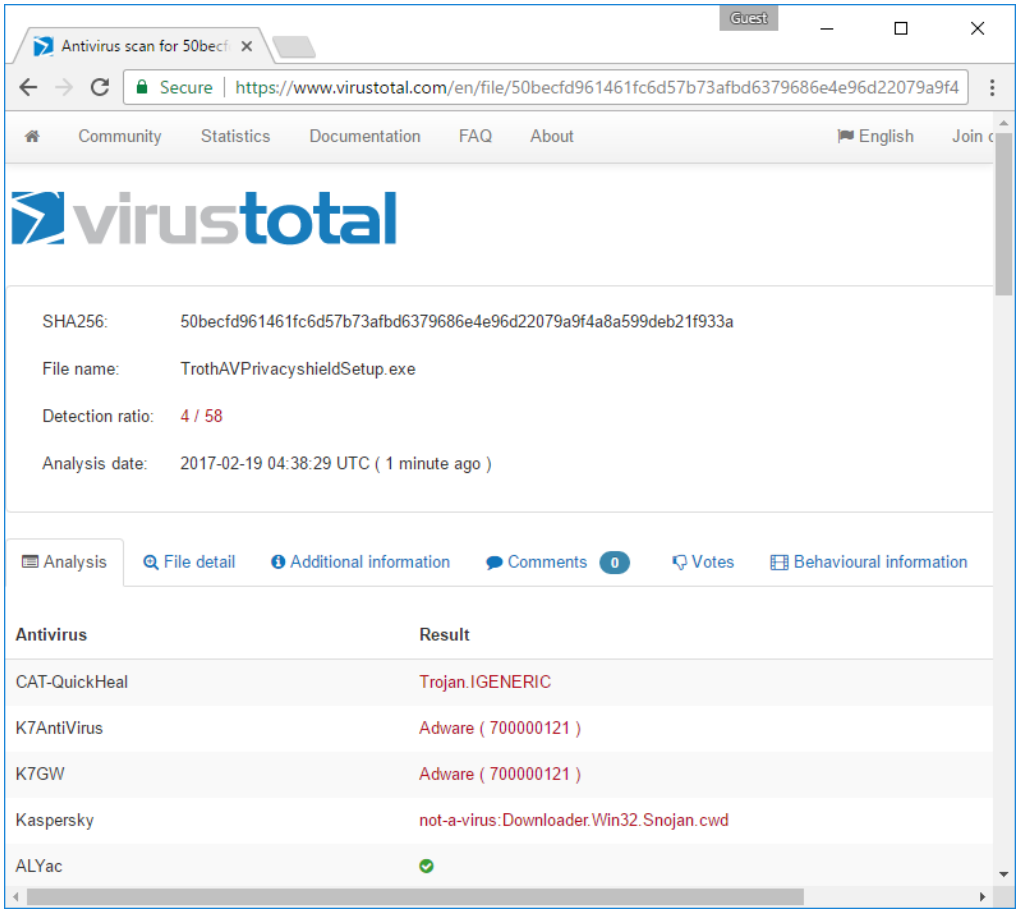


*Figure 3. Troth Privacy Shield marked as malware by four popular antivirus products.*

23. Finally, the installation of ad-blockers may cause usability issues to certain users. Many websites (especially those that depend on ad revenue, like Forbes.com and Hulu.com) detect the presence of ad blockers and request their users to disable them in order to continue browsing. If a consumer is not aware that he is running an ad-blocker (and likely does not know how to disable one), the consumer may not be able to browse such websites.

24. Overall, while the majority of the services provided by Troth Solutions were not malicious, consent for the purchase of these services was obtained using a misleading infection narrative that is not representative of the true state of the investigator's computer. Indeed, nothing done by the Troth Solutions representatives gave them the necessary information to make their diagnoses and recommendations. An analogy for

what the representative did would be for a car mechanic to diagnose a car's faulty brakes by inspecting the car's air conditioning, and then charge the customer for the completely unnecessary replacement of his brakes with new brakes.

**POP UP Analysis**

25. I have developed a custom internet crawler that, on a daily basis, identifies technical support scam domains and keeps a record of them in its database. This tool has been in operation since September 30, 2015. FTC staff shared with me, on January 12, 2017, a list of domains, phone-numbers, and keywords associated with their investigation in Troth Solutions.

26. Among the results of my tool, there were two entries for technical support scam popups that were located on the domains techquickbooksupport.com and quickbooknumber.com. According to WHOIS records, both of these domains are registered by "madhu sethi" with an address that I understand from FTC staff is Mr. Sethi's residence in Boca Raton, Florida.

27. My tool was able to identify popups located on these two specific URLs on October 6 and October 8, 2016:

    - http://techquickbooksupport.com/ads-popup/index.html?tfn=8554117582&ftfn=(800)-797-5365&a=true
    - http://quickbooknumber.com/ads-popup/index.html?tfn=8554117582&ftfn=(800)-797-5365&a=true

These domains belong to the owners of Troth Solutions (as identified to me by FTC staff) and they are hosted on a webserver (IP address: 192.186.236.119) which hosts domains associated with services owned by the owners of Troth Solutions (e.g., qkontos.com, trothav.com, trothsolutions.com, applehelp-number.com). In other words, the content hosted on these websites is fully under the control of the owners of Troth Solutions.

28. The popups that were served from these locations were warning users that their computer was breached by "ROOTKIT_TROJAN_HIJACK.EXE", that their "Windows Defender" software was unable to load and that the "health" of their Windows system was "critical." *Figure 4* shows a partial reconstruction of what these popups would look like to consumers, based on the HTML code that my tool was able to locate and store. The warnings contained in these popups are completely false for the following two reasons:

    - My tool is running on a Linux operating system with a web browser that only pretends to be one running on Windows. The Linux operating system does not support the Windows Defender program and it cannot execute .EXE programs.
    - By design, web browsers do not expose programmatic interfaces which websites could tap in to obtain information about a computer's filesystem, registry, running programs, etc. Therefore, from a technical point of view, websites cannot identify

whether a user has a virus running on his computer. They would have to prompt the user to download software which would run outside of the browser and retrieve this information. This was not done in this case, therefore I can again confidently state that the warnings in these popups are fake statements meant to scare a user into calling the phone number listed on these webpages.


*Figure 4. Reconstruction of what the popups from techquickbooksupport.com and quickbooknumber.com looked like*

29. The "BSOD" reference in this popup is to something commonly called the "blue screen of death." A "blue screen of death" is normally shown to users of the Windows operating system, when the system experiences an error from which it cannot recover. These unrecoverable errors are typically associated with faulty drivers and faulty hardware. Consumers who have seen these error screens before are likely to mistake this popup as an important warning from their operating system and thus act upon it. Note that

legitimate “blue screen of death” warnings never include a phone number. They only include information that a consumer could write down to later show to a technician who is attempting to diagnose the problem that caused the “blue screen of death” warning to be showed.

30. In addition to the deceptive messages, the popup pages served from techquickbooksupport.com and quickbooknumber.com were using intrusive JavaScript techniques to hijack a user’s browser making it near impossible for non-technical users to be able to close the popups or navigate to a different website. Whenever users moved their mouse, clicked on the page, tried to type, or tried to navigate away, the popup page instructed the user’s browser to execute a JavaScript function called “myFunction”. That function would create a barrage of alert messages (small dialogue boxes, supported by modern browsers, which are meant to communicate something important to users) with more fake security messages in an effort to stop users from navigating away and to further convince them to call the listed number. Moreover, the same code would attempt to constantly open new tabs in a user’s browser to show again the same popup with the same warnings. Figure 5 shows part of this code and the sections relevant to fake warning messages, the launching of new popups and the calling of this function over and over again (launching new warnings and popups every 100 milliseconds). This practice, often referred to as “browser hijacking,” is a technique commonly used in “malvertising,” a term coined to describe the way computer users are often exposed to multiple attacks, including technical support scams, through malware-infected online advertising.


*Figure 5. Part of the JavaScript code of the popup served from techquickbooksupport.com and quickbooknumber.com. The code includes the type of messages shown to users and the mechanisms for launching these alerts and popups over and over again.*

31. I am willing to travel within the United States to testify in any court action concerning the above-stated matters.

I declare, under penalty of perjury, that the foregoing statement is true and correct.

Executed on 4/19/2017

Nikolaos Nikiforakis

# Nick Nikiforakis

*Curriculum Vitae*

*Department of Computer Science*
*Stony Brook University*
*Stony Brook , NY 11794-2424*
☎ *(631) 632 2464*
✉ *nick@cs.stonybrook.edu*
*www.securitee.org*

## Research Interests

Web Security and Privacy, Software Security, Intrusion Detection, Cybercrime

## Employment

Aug 2014 – Present **Assistant Professor**, *Department of Computer Science*, Stony Brook University.

2013–2014 **Postdoctoral Researcher**, *Department of Computer Science*, KU Leuven, Belgium.

Jun - Sep 2012 **Research Visitor**, *Department of Computer Science*, University of California, Santa Barbara.

## Education

2009–2013 **Ph.D. in Computer Science**,
*Computer Science Department*, KU Leuven, Belgium.

thesis *Towards a Secure Web: Critical Vulnerabilities and Client-Side Countermeasures*

supervisors Prof. Wouter Joosen and Prof. Frank Piessens

2007–2009 **M.Sc. in Parallel and Distributed Systems**,
*Computer Science Department*, University of Crete, Greece.

thesis *Parasitic Storage: Free and globally accessible gigabytes*

supervisor Professor Evangelos Markatos

2003–2007 **B.Sc. in Computer Science**,
*Computer Science Department*, University of Crete, Greece.

thesis *Handling real-time network data generated by network-monitoring applications*

supervisor Professor Evangelos Markatos

## Teaching Experience

| | |
|---|---|
| Fall 2016 | Instructor, CSE509 System Security, Stony Brook University |
| Spring 2016 | Instructor, CSE659 Computer Security Seminar, Stony Brook University |
| Fall 2015 | Instructor, CSE509 System Security, Stony Brook University |
| Spring 2015 | Instructor, CSE508 Network Security, Stony Brook University |
| Fall 2014 | Instructor, CSE509 System Security, Stony Brook University |
| Fall 2013 | Teaching Assistant, Secure Software for Athens 2013, KU Leuven |
| Spring 2013 | Teaching Assistant, Capita Selecta Secure Software, KU Leuven |
| Fall 2011 | Teaching Assistant, Capita Selecta Secure Software, KU Leuven |
| Fall 2010 | Teaching Assistant, Capita Selecta Secure Software, KU Leuven |
| Fall 2008 | Teaching Assistant, CS557 - Secure Systems, University of Crete |
| Spring 2008 | Teaching Assistant, CS455 - Lab for Network Attacks and Defenses, University of Crete. |
| Fall 2007 | Teaching Assistant, CS345 - Operating Systems, University of Crete |

## Work Experience

**2014 – present** As an Assistant Professor at Stony Brook University, I teach security-related courses, advise Ph.D. and M.Sc. students, write and review academic and industry grants, write and review papers for the top conferences and journals of my field, and participate in administrative activities, such as the reviewing of Ph.D. and M.Sc. admissions.

**2013 – 2014** As a Postdoctoral Researcher at KU Leuven, I continued the empirical exploratory security and privacy research, while coaching young graduate students.

**2009 – 2013** During my PhD at KU Leuven, I had the opportunity to successfully coach the theses of four Master students, teach the "Hands-on Hacking" module of the Capita Selecta Secure Software course, and do research on many areas, relevant to security, such as software security, web security, and privacy.

**Jun – Sep 2012** I visited Prof. Christopher Kruegel and Prof. Giovanni Vigna for 3 months at the University of California, Santa Barbara and worked in the Computer Security Lab on web-based device fingerprinting.

**2006 – 2009** I worked as a Research Assistant at the Distributed Computing Systems Lab of FORTH-ICS in Heraklion. I participated in three EU-funded programs: LOBSTER (Large-scale Monitoring of Broadband Internet Infrastructures), MOMENT (Monitoring and Measurement in the Next Generation Technologies), and NoAH (Network of Affined Honeypots).

## Grants

- *TWC: Small: Combating Environment-aware Malware* (2016.09 – 2019.08)
  - PI: Michail Polychronakis, co-PI: Nick Nikiforakis, Sponsor: National Science Foundation, Amount: $498,036
- *TWC: Small: Emerging Attacks Against the Mobile Web and Novel Proxy Technologies for Their Containment* (2016.09 – 2019.08)
  - PI: Nick Nikiforakis, co-PI: Nima Honarmand, Sponsor: National Science Foundation, Amount: $499,481
- *Early Detection of User-impersonating Attackers using Multilayer Tripwires* (2016.03 – 2019.02)
  - PI: Nick Nikiforakis, co-PI: Erez Zadok, Sponsor: Office of Naval Research, Amount: $586,215
- *TWC: Small: Cross-application and Cross-platform Tracking of Web Users: Techniques and Countermeasures* (2015.09 – 2018.08)
  - PI: Nick Nikiforakis, co-PI: Long Lu, Sponsor: National Science Foundation, Amount: $499,204
- *Understanding and defending against technical support scams* (2015.07 – 2015.12)
  - PI: Nick Nikiforakis, Sponsor: Cyber Research Institute, Amount: $67,000
- *Grant for teaching network security* (2015.02)
  - PI: Nick Nikiforakis, Sponsor: Amazon Web Services, Amount: $8,600
- *Grant for conducting cloud experiments* (2014.02)
  - PI: Nick Nikiforakis, Sponsor: Linode, Amount: $2,000

## Awards

- Distinguished Paper Award at NDSS 2017
- Graduate Teaching Award, Department of Computer Science, Stony Brook University, 2016
- Honorable Mention at PETS 2016
- Best Paper Award at ISC 2014

## Public Service

### Program Chair

- Symposium on Electronic Crime Research (eCrime 2017), co-chair with Damon McCoy
- OWASP Application Security Conference, Research Track (OWASP AppSecEU 2015)

### Publicity Chair

- 20th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2017)

### Member of Program Committees

- 24th ACM Conference on Computer and Communications Security (CCS 2017)
- 2nd European Workshop on Usable Security (EuroUSEC 2017)
- 26th USENIX Security Symposium (USENIX Security 2017)
- 14th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2017)

- 7th ACM Conference on Data and Application Security and Privacy (CODASPY 2017)
- 25th International World Wide Web Conference (WWW 2017)
- 2nd IEEE European Symposium on Security and Privacy (EuroS&P 2017)
- 16th ACM Symposium on Applied Computing (SAC 2017)
- 32nd Annual Computer Security Applications Conference (ACSAC 2016)
- 23rd ACM Conference on Computer and Communications Security (CCS 2016)
- 25th USENIX Security Symposium (USENIX Security 2016)
- 11th Symposium on Electronic Crime Research (eCrime 2016)
- 13th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2016)
- 6th ACM Conference on Data and Application Security and Privacy (CODASPY 2016)
- 8th International Symposium on Engineering Secure Software and Systems (ESSoS 2016)
- 22nd ACM Conference on Computer and Communications Security (CCS 2015)
- 24th USENIX Security Symposium (USENIX Security 2015)
- 8th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec 2015)
- 12th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2015)
- 24th International World Wide Web Conference (WWW 2015)
- 8th European Workshop on System Security (EuroSec 2015)
- 7th International Symposium on Engineering Secure Software and Systems (ESSoS 2015)
- 7th European Workshop on System Security (EuroSec 2014)
- 5th International Conference on Emerging Ubiquitous Systems and Pervasive Member of Networks (EUSPN 2014)
- 12th IEEE International Conference on Embedded and Ubiquitous Computing (EUC 2014)
- 7th IEEE Workshop on Network Measurements (IEEE WNM 2013)
- 4th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2013)
- OWASP AppSec Europe 2013 - Research Track (AppSec 2013)
- 6th European Workshop on System Security (EuroSec 2013)
- 14th IFIP Conference on Communications and Multimedia Security (CMS 2013)
- 5th European Workshop on System Security (EuroSec 2012)
- 13th IFIP Conference on Communications and Multimedia Security (CMS 2012)

## Invited Talks

| | |
|---|---|
| Mar 2017 | CyLab Distinguished Seminar – Dial One for Scam - A Large-Scale Analysis of Technical Support Scams |
| Jan 2017 | Federal Trade Commission, Washington DC – Dial One for Scam - A Large-Scale Analysis of Technical Support Scams |
| Feb 2016 | Messaging, Malware and Mobile Anti-Abuse Working Group – No Honor Among Thieves: A Large-Scale Analysis of Malicious Web Shells |
| May 2015 | International World Wide Web Conference, W3C Track: Web Security Architecture – The Pretense of Security |

Oct 2014 Princeton Web Privacy and Transparency Conference – Web-based Device Fingerprinting

Feb 2014 SecAppDev – Browser fingerprinting (how did we get here?), Leuven, Belgium

Dec 2013 Microsoft Research – Everything you always wanted to know about web-based device fingerprinting (but were afraid to ask), Redmond, Washington, US

Nov 2013 November OWASP BeNeLux – Everything you always wanted to know about web-based device 2013 fingerprinting (but were afraid to ask), Amsterdam, The Netherlands

Jul 2013 SysSec Workshop – Cookieless Monster: Exploring the Ecosystem of Web-based Device Fingerprinting, Bochum, Germany

Feb 2013 SecAppDev – Sandboxing JavaScript, Leuven, Belgium

Oct 2012 Web Application Security Seminar Dagstuhl – You are what you include: Large-scale analysis of remote JavaScript inclusions, Bochum, Germany

Jul 2011 OWASP Netherlands Chapter – Abusing locality in Shared Web Hosting, Amsterdam, The Netherlands

Dec 2010 OWASP BeNeLux – On the Privacy of File Sharing Services, Eindhoven, The Netherlands

## Selected Media Coverage

Mar 2017 WIRED – Listen to "Tech Support" Scam Calls That Bilk Victims Out of Millions – `https://www.wired.com/2017/03/listen-tech-support-scam-calls-bilk-millions-victims/`

Jun 2016 Washington Times – Half the ads on livestreaming sites pose security risks to viewers: Report – `http://www.washingtontimes.com/news/2016/jun/15/half-ads-livestreaming-sites-pose-security-risks-v/`

Feb 2016 BBC – Illegal football streams are 'dangerous', study says – `http://www.bbc.com/news/technology-35434765`

Dec 2015 TechRepublic – DDoS mitigation may leave your site vulnerable – `http://www.techrepublic.com/article/ddos-mitigation-may-leave-your-site-even-more-vulnerable/`

Oct 2015 The Register – DDoS defences spiked by CloudPiercer tool - paper – `http://www.theregister.co.uk/2015/10/08/cloudpiercer_tool_lifts_ddos_protection_cloak_from_70_percent_of_sites/`

Oct 2015 SC Magazine – CloudPiercer tool discloses DDoS defence providers – `http://www.scmagazineuk.com/cloudpiercer-tool-discloses-ddos-defence-providers/article/444000/`

Sep 2015 KrebsOnSecurity – With Stolen Cards, Fraudsters Shop to Drop – `http://krebsonsecurity.com/2015/09/with-stolen-cards-fraudsters-shop-to-drop/`

Sep 2015 SlashDot – Study: $1.8 Billion In Reshipping Fraud With Stolen Cards Each Year –http://news.slashdot.org/story/15/09/28/2157238/study-18-billion-in-reshipping-fraud-with-stolen-cards-each-year

Feb 2015 World Trademark Review – Groundbreaking typosquatting research reveals true scale of the problem – http://www.worldtrademarkreview.com/Blog/Detail.aspx?g=59f40171-11fb-4806-a837-2c0b29564681

Jan 2015 HelpNet Security – Typosquatting abuse of 500 most popular websites analyzed – http://www.net-security.org/secworld.php?id=17833

Dec 2014 ArsTechnica – Sites certified as secure often more vulnerable to hacking, scientists find – http://www.arstechnica.com/security/2014/12/sites-certified-as-secure-often-morevulnerable-to-hacking-scientists-find/

## Magazine Articles

Jan 2015 IEEE IT Pro – Protected Web Components: Hiding Sensitive Information in the Shadows

Aug 2014 IEEE Spectrum – Browse at your own risk

Dec 2013 IEEE Security & Privacy – On the Workings and Current Practices of Web-based Device Fingerprinting

Mar 2011 Hackin9 – Direct Object Reference or, How a Toddler Can Hack Your Web Application

## Publications

[1] Oleksii Starov and Nick Nikiforakis. XHOUND: Quantifying the Fingerprintability of Browser Extensions. In *Proceedings of the 38th IEEE Symposium on Security and Privacy (IEEE S&P)*, 2017.

[2] Najmeh Miramirkhani, Mahathi Priya Appini, Nick Nikiforakis, and Michalis Polychronakis. Spotless Sandboxes: Evading Malware Analysis Systems using Wear-and-Tear Artifacts. In *Proceedings of the 38th IEEE Symposium on Security and Privacy (IEEE S&P)*, 2017.

[3] Oleksii Starov and Nick Nikiforakis. Extended Tracking Powers: Measuring the Privacy Diffusion Enabled by Browser Extensions. In *Proceedings of the 26th International World Wide Web Conference (WWW)*, 2017.

[4] Enrico Mariconti, Jeremiah Onaolapo, Syed Sharique Ahmad, Nicolas Nikiforou, Manuel Egele, Nick Nikiforakis, and Gianluca Stringhini. What's in a Name? Understanding Profile Name Reuse on Twitter. In *Proceedings of the 26th International World Wide Web Conference (WWW)*, 2017.

[5] Najmeh Miramirkhani, Oleksii Starov, and Nick Nikiforakis. Dial One for Scam: A Large-Scale Analysis of Technical Support Scams. In *Proceedings of the 24th Network and Distributed System Security Symposium (NDSS)*, 2017.

[6] Georg Merzdovnik, Markus Huber, Damjan Buhov, Nick Nikiforakis, Sebastian Neuner, Martin Schmiedecker, and Edgar Weippl. Block Me If You Can: A Large-Scale Study of Tracker-Blocking Tools. In *Proceedings of the 2nd IEEE European Symposium on Security and Privacy (IEEE EuroS&P)*, 2017.

[7] Enrico Mariconti, Jeremiah Onaolapo, Syed Sharique Ahmad, Nicolas Nikiforou, Manuel Egele, Nick Nikiforakis, and Gianluca Stringhini. Why Allowing Profile Name Reuse Is A Bad Idea. In *Proceedings of the 9th European Workshop on System Security (EUROSEC)*, 2016.

[8] Oleksii Starov, Johannes Dahse, Syed Sharique Ahmad, Thorsten Holz, and Nick Nikiforakis. No Honor Among Thieves: A Large-Scale Analysis of Malicious Web Shells. In *Proceedings of the 25th International World Wide Web Conference (WWW)*, 2016.

[9] Zubair Rafique, Tom Van Goethem, Wouter Joosen, Christophe Huygens, and Nick Nikiforakis. It's Free for a Reason: Exploring the Ecosystem of Free Live Streaming Services. In *Proceedings of the 23rd Network and Distributed System Security Symposium (NDSS)*, 2016.

[10] Oleksii Starov, Phillipa Gill, and Nick Nikiforakis. Are You Sure You Want to Contact Us? Quantifying the Leakage of PII via Website Contact Forms. In *Proceedings of the 16th Privacy Enhancing Technologies Symposium (PETS)*, 2016.

[11] Tom Van Goethem, Wouter Joosen, and Nick Nikiforakis. The Clock is Still Ticking: Timing Attacks in the Modern Web. In *Proceedings of the 22nd ACM Conference on Computer and Communications Security (CCS)*, 2015.

[12] Thomas Vissers, Tom Van Goethem, Wouter Joosen, and Nick Nikiforakis. Maneuvering Around Clouds: Bypassing Cloud-based Security Providers. In *Proceedings of the 22nd ACM Conference on Computer and Communications Security (CCS)*, 2015.

[13] Shuang Hao, Kevin Borgolte, Nick Nikiforakis, Gianluca Stringhini, Manuel Egele, Mike Eubanks, Brian Krebs, and Giovanni Vigna. Drops for Stuff: An Analysis of Reshipping Mule Scams. In *Proceedings of the 22nd ACM Conference on Computer and Communications Security (CCS)*, 2015.

[14] Nick Nikiforakis, Wouter Joosen, and Benjamin Livshits. PriVaricator: Deceiving Fingerprinters with Little White Lies. In *Proceedings of the 24th International World Wide Web Conference (WWW)*, 2015.

[15] Thomas Vissers, Wouter Joosen, and Nick Nikiforakis. Parking Sensors: Analyzing and Detecting Parked Domains. In *Proceedings of the 22nd Network and Distributed System Security Symposium (NDSS)*, 2015.

[16] Pieter Agten, Wouter Joosen, Frank Piessens, and Nick Nikiforakis. Seven Months' Worth of Mistakes: A Longitudinal Study of Typosquatting Abuse. In *Proceedings of the 22nd Network and Distributed System Security Symposium (NDSS)*, 2015.

[17] Nick Nikiforakis, Marco Balduzzi, Lieven Desmet, Frank Piessens, and Wouter Joosen. Soundsquatting: Uncovering the use of homophones in domain squatting. In *Proceedings of the 17th Information Security Conference (ISC)*, 2014.

[18] Tom Van Goethem, Frank Piessens, Wouter Joosen, and Nick Nikiforakis. Clubbing Seals: Exploring the Ecosystem of Third-party Security Seals. In *Proceedings of the 21st ACM Conference on Computer and Communications Security (CCS)*, pages 918–929, 2014.

[19] Ping Chen, Nick Nikiforakis, Lieven Desmet, and Christoph Huygens. Security Analysis of the Chinese Web: How well is it protected? In *the Workshop of Cyber Security Analytics and Automation (SafeConfig)*, 2014.

[20] Thomas Vissers, Nick Nikiforakis, Nataliia Bielova, and Wouter Joosen. Crying Wolf? On the Price Discrimination of Online Airline Tickets. In *the 7th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs)*, 2014.

[21] Tom Van Goethem, Ping Chen, Nick Nikiforakis, Lieven Desmet, and Wouter Joosen. Large-scale Security Analysis of the Web: Challenges and Findings. In *Proceedings of the 7th International Conference on Trust & Trustworthy Computing (TRUST)*, pages 110–126, 2014.

[22] Steven Van Acker, Nick Nikiforakis, Lieven Desmet, Frank Piessens, and Wouter Joosen. Monkey-in-the-browser: Malware and vulnerabilities in augmented browsing script markets. In *Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security (ASIACCS)*, 2014.

[23] Nick Nikiforakis, Federico Maggi, Gianluca Stringhini, M Zubair Rafique, Wouter Joosen, Christopher Kruegel, Frank Piessens, Giovanni Vigna, and Stefano Zanero. Stranger danger: exploring the ecosystem of ad-based url shortening services. In *Proceedings of the 23rd International World Wide Web Conference (WWW)*, pages 51–62, 2014.

[24] Ping Chen, Nick Nikiforakis, Lieven Desmet, and Christophe Huygens. A Dangerous Mix: Large-scale analysis of mixed-content websites. In *Proceedings of the 16th Information Security Conference (ISC)*, 2013.

[25] Gunes Acar, Marc Juarez, Nick Nikiforakis, Claudia Diaz, Seda Gürses, Frank Piessens, and Bart Preneel. Fpdetective: Dusting the web for fingerprinters. In *Proceedings of the ACM SIGSAC Conference on Computer & Communications Security (CCS)*, pages 1129–1140, 2013.

[26] Nick Nikiforakis, Frank Piessens, and Wouter Joosen. HeapSentry: Kernel-assisted Protection against Heap Overflows. In *Proceedings of the 10th Conference on Detection of Intrusions and Malware & Vulnerability Analysis (DIMVA)*, pages 177–196, 2013.

[27] Nick Nikiforakis, Steven Van Acker, Wannes Meert, Lieven Desmet, Frank Piessens, and Wouter Joosen. Bitsquatting: Exploiting bit-flips for fun, or profit? In *Proceedings of the 22nd International World Wide Web Conference (WWW)*, pages 989–998, 2013.

[28] Nick Nikiforakis, Alexandros Kapravelos, Wouter Joosen, Christopher Kruegel, Frank Piessens, and Giovanni Vigna. Cookieless monster: Exploring the ecosystem of web-based

device fingerprinting. In *Proceedings of the 34th IEEE Symposium on Security and Privacy (IEEE S&P)*, pages 541–555, 2013.

[29] Philippe De Ryck, Nick Nikiforakis, Lieven Desmet, and Wouter Joosen. Tabshots: Client-side detection of tabnabbing attacks. In *Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security (AsiaCCS)*, pages 447–455, May 2013.

[30] Willem De Groef, Dominique Devriese, Nick Nikiforakis, and Frank Piessens. FlowFox: a Web Browser with Flexible and Precise Information Flow Control. In *Proceedings of the 19th ACM Conference on Computer and Communications Security (CCS)*, pages 748–759, 2012.

[31] Nick Nikiforakis, Luca Invernizzi, Alexandros Kapravelos, Steven Van Acker, Wouter Joosen, Christopher Kruegel, Frank Piessens, and Giovanni Vigna. You Are What You Include: Large-scale Evaluation of Remote JavaScript Inclusions. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, pages 736–747, 2012.

[32] Job Noorman, Nick Nikiforakis, and Frank Piessens. There is Safety in Numbers: Preventing Control-Flow Hijacking by Duplication. In *Proceedings of the 17th Nordic Conference on Secure IT Systems (NordSec)*, 2012.

[33] Sebastian Lekies, Nick Nikiforakis, Walter Tighzert, Frank Piessens, and Martin Johns. DEMACRO: Defense against Malicious Cross-domain Requests. In *Proceedings of the 15th International Symposium on Research In Attacks, Intrusions and Defenses (RAID)*, pages 254–273, 2012.

[34] Philippe De Ryck, Nick Nikiforakis, Lieven Desmet, Frank Piessens, and Wouter Joosen. Serene: Self-reliant client-side protection against session fixation. In *Proceedings of 12th IFIP International Conference on Distributed Applications and Interoperable Systems (DAIS)*, pages 59–72. Springer, 2012.

[35] Nick Nikiforakis, Steven Van Acker, Frank Piessens, and Wouter Joosen. Exploring the Ecosystem of Referrer-Anonymizing Services. In *Proceedings of the 12th Privacy Enhancing Technology Symposium (PETS)*, pages 259–278, 2012.

[36] Pieter Agten, Nick Nikiforakis, Raoul Strackx, Willem De Groef, and Frank Piessens. Recent Developments in Low-Level Software Security. In *Proceedings of the 6th Workshop in Information Security Theory and Practice (WISTP)*, 2012.

[37] Steven Van Acker, Nick Nikiforakis, Lieven Desmet, Wouter Joosen, and Frank Piessens. FlashOver: Automated Discovery of Cross-site Scripting Vulnerabilities in Rich Internet Applications. In *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security (ASIACCS)*, 2012.

[38] Francesco Gadaleta, Nick Nikiforakis, Jan Tobias Muhlberg, and Wouter Joosen. HyperForce: Hypervisor-enForced Execution of Security-Critical Code. In *Proceedings of the 27th IFIP International Information Security and Privacy Conference (IFIP SEC)*, 2012.

[39] John Wilander, Nick Nikiforakis, Yves Younan, Mariam Kamkar, and Wouter Joosen. RIPE: Runtime Intrusion Prevention Evaluator. In *In Proceedings of the 27th Annual Computer Security Applications Conference, (ACSAC)*, pages 41–50, 2011.

[40] Francesco Gadaleta, Nick Nikiforakis, Yves Younan, and Wouter Joosen. Hello rootKitty: A lightweight invariance-enforcing framework. In *Proceedings of the 14th Information Security Conference (ISC)*, 2011.

[41] Nick Nikiforakis, Marco Balduzzi, Steven Van Acker, Wouter Joosen, and Davide Balzarotti. Exposing the lack of privacy in file hosting services. In *Proceedings of the 4th USENIX conference on Large-scale exploits and emergent threats (LEET)*, 2011.

[42] Nick Nikiforakis, Wouter Joosen, and Martin Johns. Abusing Locality in Shared Web Hosting. In *Proceedings of the 4th European Workshop on System Security (EuroSec)*, pages 2:1–2:7, 2011.

[43] Nick Nikiforakis, Wannes Meert, Yves Younan, Martin Johns, and Wouter Joosen. SessionShield: Lightweight Protection against Session Hijacking. In *Proceedings of the 3rd International Symposium on Engineering Secure Software and Systems (ESSoS)*, pages 87–100, 2011.

[44] Steven Van Acker, Nick Nikiforakis, Pieter Philippaerts, Yves Younan, and Frank Piessens. ValueGuard: Protection of native applications against data-only buffer overflows. In *Proceedings of the Sixth International Conference on Information Systems Security (ICISS)*, 2010.

[45] Nick Nikiforakis, Yves Younan, and Wouter Joosen. HProxy: Client-side detection of SSL stripping attacks. In *Proceedings of the 7th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)*, pages 200–218, 2010.

[46] Demetris Antoniades, Michalis Polychronakis, Nick Nikiforakis, Evangelos P. Markatos, and Yiannis Mitsos. Monitoring three National Research Networks for Eight Weeks: Observations and Implications. In *6th IEEE Workshop on End-to-End Monitoring Techniques and Services (E2EMon)*, 2008.

[47] Nikos Nikiforakis, Andreas Makridakis, Elias Athanasopoulos, and Evangelos P Markatos. Alice, What Did You Do Last Time? Fighting Phishing Using Past Activity Tests. In *Proceedings of the 3rd European Conference on Computer Network Defense (EC2ND)*, pages 107–117, 2007.